UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/905,532	07/14/2001	Antony John Rogers	063170.6291	3485

5073 7590 10/31/2005

BAKER BOTTS L.L.P.
2001 ROSS AVENUE
SUITE 600
DALLAS, TX 75201-2980

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/31/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/905,532	ROGERS ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,8-17 and 20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8-17 and 20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-5,8-17, and 20 have been considered.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/22/05 has been entered.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5 and 10-17 are rejected under 35 U.S.C. 102(b) as being anticipated by Chambers, U.S. Patent No. 5,398,196.

As per claims 1,10,11,12, and 14, the applicant discloses the following method of detecting viral code which is anticipated by Chambers:

a) creating an artificial memory region spanning one or more components of the operating system (Col 7, line 63 to Col 8, line 21; Col 7, lines 23-28);

b) creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values (Col 9, lines 13-32);

c) emulating execution of computer executable code in a subject file (Col 3, lines 42-45);

d) detecting when the emulated computer executable code attempts to access the artificial memory region (Col 8, lines 28-30);

As per claim 2, the applicant discloses the method of claim 1, which is met by Chambers (see above), with the following limitation which is also met by Chambers:

Wherein detecting when the emulated computer executable code attempts to access the artificial memory region comprises monitoring operating system calls by the emulated computer executable code (Col 6, line 68; Col 7, lines 1-15).

As per claim 3, the applicant discloses the method of claim 1, which is met by Chambers (see above), with the following limitations which are also met by Chambers:

a) determining an operating system call that the emulated computer executable code attempted to access (Col 9, lines 13-25; Col 9, lines 44-54);

b) monitoring the operating system call to determine whether the computer executable code is viral (Col 9, lines 13-25; Col 9, lines 44-54).

The applicant should note that the operating system call is the attempt to gain access to an operating system entry point. Through emulation of an interrupt handler routine, the method is able to monitor whether a virus is present.

As per claims 4 and 16, the applicant discloses the method of claim 1, which is met by Chambers (see above), with the following limitations which are also met by Chambers:

a) determining an operating system call that the emulated computer executable code attempted to access (Col 9, lines 13-25; Col 9, lines 44-54);

b) emulating functionality of the operating system call while monitoring the operating system call to determine whether the computer executable code is viral (Col 9, lines 13-25; Col 9, lines 44-54);

The applicant should note that the operating system call is the attempt to gain access to an operating system entry point. Through emulation of an interrupt handler routine, the method is able to monitor whether a virus is present.

As per claims 5 and 17, the applicant discloses the method of claim 1, which is met by Chambers (see above), with the following limitations which are also met by Chambers:

a) monitoring accesses by the emulated computer executable code to the artificial memory region to detect looping (Col 3, lines 51-53; Col 3, line 64 to Col 4, line 14);

b) determining based on a detection of looping whether the emulated computer executable code is viral (Col 3, lines 51-53; Col 3, line 64 to Col 4, line 14).

As per claims 13 and 15, the applicant discloses the method of claims 12 and 14 respectively, which are met by Chambers (see above), with the following limitations which are also met by Chambers:

a) a fourth segment comprising auxiliary code, wherein the auxiliary code determines an operating system call that the emulated computer executable code attempted to access (Col 9, lines 13-25; Col 9, lines 44-54);

b) a fifth segment comprising analyzer code, wherein the analyzer code monitors the operating system call to determine whether the computer executable code is viral, while emulation continues (Col 9, lines 13-25; Col 9, lines 44-54);

The applicant should note that the monitor described in the passages listed for a) and b) above could be deemed as auxiliary or analyzer code. The operating system call is the attempt to gain access to an operating system entry point.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8,9, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chambers in further view of Golan, U.S. Patent No. 5,974,549.

As per claim 8, the applicant describes the method of claim 1, which is anticipated by Chambers (see above), with the following limitation which is anticipated by Golan:

Further comprising monitoring access by the emulated computer executable code to dynamically linked functions (Col 6, lines 6-12; Col 5, lines 60-63);

Chambers describes all the limitations of claim 1, the independent claim. However, Chambers fails to disclose anything concerning dynamically linked functions. Golan describes a security monitor method whereby access to dynamically linked functions is regulated because, as Golan discloses, "in an operating system that supports virtual memory and hardware abstraction, a software component can only breach security by calling a system call" (Col 5, lines 38-41). It would have been obvious to one of ordinary skill in that art at the time the invention was filed to have combined the teachings of Chambers with those of Golan and monitor access to dynamically linked functions because requesting access to dynamically linked functions could be an attempt to breach security.

As per claim 9, the applicant discloses the method of claim 8, which is met by Chambers in further view of Golan (see above), with the following limitation which is met by Golan:

Wherein the artificial memory region spans a jump table containing pointers to the dynamically linked functions (Col 7, lines 31-35);

Chambers in further view of Golan describes all the limitations of claim 8. Golan describes the additional limitation of a jump table containing pointers to the dynamically linked functions. The jump table is often incorporated with dynamically linked functions to store the actual addresses of the

dynamically linked functions. It would have been obvious to one of ordinary skill in the art at the time in the invention was filed to have included a jump table with the method so that there could be a way of storing the actual addresses of the dynamically linked functions.

As per claim 20, the applicant discloses the method of claim 14, which is met by Chambers (see above), with the following limitation which is met by Golan:

Wherein the artificial memory region created by the memory manager component spans a jump table containing pointers to dynamically linked functions, and the monitor component monitors access by the emulated computer executable code to the dynamically linked functions;

The claim is met by the combination of claims 8 and 9. Explanations for claim 8 and 9 rejections are listed above.

Response to Arguments

Applicant's arguments filed 9/22/05 with respect to claim 1 have been fully considered but they are not persuasive. The applicant argues that the following amended limitation is not present in Chambers:

"Creating a custom version of an export table, wherein the custom version of the export table is associated with a plurality of entry points and wherein the entry points comprise predetermined values"

The examiner has stated in the previous two actions that Chambers discloses a list which contains a plurality of entry points and wherein these entry points comprise predetermined values (See Chambers: Col 9, lines 13-32). In response, the applicant argues that the entry points do not comprise predetermined values:

"Chambers does not indicate that the list of operating system entry points 'comprise[s] predetermined values'. Thus Chambers fails to disclose any "export table [that] is associated with a plurality of entry points [wherein] the entry points comprise predetermined values'" (See Applicant's Remarks: page 2).

The examiner respectfully disagrees with the applicant's assertion. As disclosed by Chambers, the entry points on the list have predetermined values. If an emulated instruction changes one of the values, it

indicates that the target program replaces an interrupt handler with a new value indicative of a routine of its own. Further, the monitor program is aware of the predetermined values of the entry points so that the monitor program can make the above detection if the target program attempts to replace a predetermined value with a new value (Chambers: Col 9, lines 20-32).

The applicant's second argument is that Chambers fails to disclose any **creation** step of the list of entry points (or export table). The examiner disagrees. The examiner fails to see how the list of entry points can exist in Chamber's system without a creation step of the list of entry points.

Applicant's arguments with respect to claim 5 have been fully considered but they are not persuasive. The examiner presents the same argument as that of the last two actions. The examiner also notes Col 3, line 64 to Col 4, line 14 of Chambers which expresses the same idea in a less circuitous manner than the passage cited in the last action. The applicant argues that Chambers does not disclose "monitoring accesses by the emulating computer executable code to the artificial memory region to detect looping" or "determining based on a detection of looping whether the emulated computer executable code is viral".

Chambers discloses the idea of monitoring accesses by the emulating computer code to a dummy program (artificial memory region) in order to detect replication behavior. This replication behavior is the process whereby emulating computer code goes through a series of instructions to copy itself to a first program (e.g. first dummy program) and the first program then goes through the series of instructions to copy itself to a second program (e.g. second dummy program), etc. This replication behavior is a looping process whereby the same set of instructions are replicatively executed. This process is indicative of a virus as the process is done in order to disseminate the viral code. Thus, if the first dummy program is emulated and found to modify a second dummy program, the monitor program can recognize that the first dummy program is trying to replicate and hence flag the original target program as viral:

> "If after modification by the target program the first dummy program is emulated and found to modify a second dummy program, then the original target program is flagged as virus infected, for having 'infected' the first dummy file with aberrant behavior" (Chambers: Col 4, lines 9-14).

Conclusion

This action is made non-final.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 7:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KS

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER